UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v. **NOTICE OF MOTION**
22-CR-6009 (CJS)(MJP)

JOHN DOUGLAS LOONEY

Defendant

MOTION BY	James A. Napier, Esq, Attorney for John Douglas Looney
DATE, TIME & PLACE	On February 27, 2023 at 1:30 pm before the Honorable Mark W. Pedersen , U.S. Courthouse, Rochester, New York
SUPPORTING PAPERS	Affirmation of James A. Napier, affirmed on February 24, 2023 the attachments hereto, and all prior proceedings had herein.
RELIEF REQUESTED	An Order granting the relief requested herein.

Dated: February 23, 2023
Rochester, New York

TO: MEGHAN MCGUIRE
ASSISTANT UNITED STATES ATTORNEY

s/James A. Napier
James A. Napier, Esq.
Attorney for John Douglas Looney
700 Powers Building
16 West Main Street
Rochester, New York 14614
585-232-4474
jim@napierandnapier.com

TO: Meghan K. McGuire, AUSA

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v. **AFFIRMATION**

22-CR-6009 (CJS) (MJP)

JOHN DOUGLAS LOONEY

Defendant

James A. Napier, Esq., attorney for John Douglas Looney, affirms as follows:

1. I am an attorney licensed to practice law in the State of New York and the United States District Court for the Western District of New York, and I represent the defendant, John Douglas Looney.

2. I am familiar with this case by reason of my investigation of this matter, conversations with my client and others, and my review of the discovery material provided to date by the government.

3. This affirmation is submitted in support of various forms of relief requested herein, and is based upon the facts as I know them, the Federal Rules of Criminal Procedure, the Federal Rules of Evidence, the United States Constitution, and other pertinent statues and law.

4. That on February 4, 2022 the government filed a Notice of Intent to Use Evidence (exhibit A), pursuant to Fed. R. Crim. P. 12(b)(4).

5. That per Fed. R. Crim. P. 12 (b) (3) (C) , defendant moves to suppress the evidence referenced in the government's notice.

6. That per Fed. R. Crim. P. 12(b) (4)(C) (3), defendant has recently retained an expert on electronic privacy law, Bonnie Burkhardt, who has conducted an exhaustive review of discovery provided to date and who has fully familiarized your affirmant with the intricacies of federal privacy law requirements regarding interception of communications. Based on the government's violations of said privacy laws in the instant case, the defendant would respectfully request the Court to consider this defense motion to suppress based on said violations of various federal privacy statutes.

INTRODUCTION

7. Freenet (the Network) is a publicly available product which provides a private file transfer service to its anonymous users. {Affidavit #5, 6, 21} The service protects the privacy of its users by encrypting content transmitted, and attempts to hide the identity of requestors. {Affidavit #21}. Defendant was using Freenet in the privacy of his home on a password-protected computer, so he had a reasonable expectation of privacy.

8. Freenet is built by software engineers, installed on computers, and was established to serve a particular purpose – to transfer files. This meets Webster's

Dictionary[1] definition of a "***facility***: *something that is built, installed, or established to serve a particular purpose.*" As such, it is protected by 18 U.S. Code § 2701.

Stored Communication Law

9. Officer Turner did not use Freenet as designed. Instead, he used a modified version of Network software, available only to sworn law enforcement officers. This modified version allows law enforcement to tap into the internals of the file transfer system and monitor network traffic. Since this modified software program can tap into information transmitted over wire and extract it for logging, the enhanced software program fits the definition of a *wiretap*. The added wiretap capability extracts IP addresses, number of peers, unique identifier assigned by the software, date/time of requests, and hash codes; then enters them into a log. {Affidavit #31-33}. This information was not voluntarily provided by the Defendant to Officer Turner, but rather private information extracted by Officer Turner using the wiretap software. Yet, Officer Turner did not obtain any Court authorization to install or operate this *wiretap* pursuant to 18 U.S. Code § 2516, thereby Officer Turner violated 18 U.S. Code § 2511. An old-fashioned wiretap is a tap on a phone line where a third party would listen and record or write a log of what transpired in the conversation. That's exactly what this software does. It listens to the network traffic and records or writes a log what transpired regarding private files transfers.

[1] Webster's Dictionary 2018 ed. https://www.merriam-webster.com/dictionary/facility

10. The extracted information details what transacted, i.e., it is a transactional record. Yet Officer Turner had no Court authorization to obtain transactional records of a private, file transfer facility, 18 U.S. Code § 2703.

11. The logging was only available to law enforcement and was not available to typical users. This additional logging exceeded the capabilities granted to general public users and thus exceeded the authorization to access the facility (Freenet) through which electronic communications service is provided, exceeding the authorization to access the facility violates 18 U.S. Code § 2701(a)(2) . Officer Turner did not request these files nor did he post the initial copy. Instead, Officer Turner monitored the intermediate internet traffic flowing through his computer, therefore, he did not qualify for the exception given in 18 U.S. Code § 2701(c)(2).

12. Since Freenet provides a private electronic (wire) file transfer service to the public, no one, including the provider of a communication service, can monitor network traffic or content transmitted through the network. The exception for monitoring is quite strict, *"... a provider of wire communication service to the public* ***shall not utilize service observing or random monitoring*** *except for mechanical or service quality control checks."* 18 U.S. Code § 2511(2)(a)(i) (emphasis added).

Interception Law

13. Officer Turner was not a service provider nor was he attempting to provide a service quality control check for the engineers of Freenet. Instead, Officer Turner described in detail how he used the modified version of the

Network software to monitor network traffic and content transmitted through the network, and gave great details about the results of this monitoring. Since Officer Turner had no court authorization to monitor content transmitted on this network, the monitoring violates 18 U.S. Code § 2511(1)(a).

14. Even if such a warrant to monitor Freenet communications was requested in Court, it would be challenged as unconstitutional for it violates Fourth Amendment rights. Similar monitoring using a geofence warrant was declared unconstitutional, *United States v. Chatrie*, No. 3:19-cr-130 (E.D. Va.). A Geofence tool scoops up the ID numbers of all cell phones within the area of a crime, around the time the crime was committed. This geofence warrant was ruled unconstitutional because it violated the Fourth Amendment rights of average citizens who happened to be in the area. Similarly, this modified version of Freenet scoops up IP addresses of average citizens who happen to be transmitting or receiving communications on Freenet. Given the same standard of law, use of this modified version of Freenet is unconstitutional.

15. Files transmitted are broken into smaller blocks for transmission. Hash code calculators are designed to check for transmission errors of a block. Each byte within a block is crunched through a formula to produce a hash code. After transmission, the same formula is applied. If the hash codes do not match, the block must be retransmitted.[2] However, law enforcement has found that hash codes can be used in other creative ways to bypass pen register, interception, and stored communication laws. Hash codes can be used to identify

[2] BitTorrent.org. *For Developers.* http://www.bittorrent.org/beps/bep_0005.html Accessed January 14, 2019.

child pornography downloaded to specific remote computers. Using hash codes from a stored communication system for a purpose other than checking for transmission errors (its designed intent) also exceeds the authority granted to general users to access the facility. 18 U.S. Code § 2701.

16. Law enforcement used hash codes to uniquely identify content transmitted. {Affidavit #61(f)}. "Content" of an electronic communication is defined to include "*any information concerning the substance, purport or meaning of that communication;*" 18 U.S. Code § 2510(8). Officer Turner obtained the hash codes so they can be used to verify content. {Affidavit #33, 61(f), 62(f), 63(f)} However, Officer Turner had no court authorization to intercept content pursuant to 18 U.S. Code § 2516. Officer Turner obtained this content by running his special modified version of the Freenet software. "Intercept" simply means to acquire the content of an electronic communication through the use of any electronic, mechanical or other device. 18 U.S. Code § 2510(4). So, Officer Turner intercepted three hash codes without any Court authorization to do so, in violation of 18 U.S. Code § 2511(1)(a).

17. The three intercepted hash codes were disclosed in the affidavit in violation of 18 U.S. Code § 2511(1)(c). The three intercepted hash codes are being used to prosecute the Defendant, in violation of 18 U.S. Code § 2511(1)(d). Any intercepted communications and evidence received in violation of the chapter may not be received in evidence and should be suppressed. 18 U.S. Code § 2515.

18. The second category of "*content*" Officer Turner obtained was the report of the probability formula used to predict what content was being transmitted and which user downloaded it. The meaning of "*content*" includes "*any information concerning the substance, purport or meaning of that communication;*" Since the formula can, allegedly, predict with 98% accuracy the substance, purport and meaning of a communication(downloader v. relayor), its report qualifies as content. Yet, Officer Turner did not obtain prior authorization to intercept content using this method, 18 U.S. Code § 2516. Therefore, running this program to obtain reports of content transmitted without any prior court authorization violates 18 U.S. Code § 2511(1)(a).

19. Officer Turner was not using Freenet in the ordinary course of business, for he was not using it as designed, to send and receive files. Instead, he used a modified version of Freenet to monitor and intercept private communications transmitted through the network. As such, Officer Turner was using the modified Freenet software as an interception device. Officer Turner's use of Freenet does not qualify for the exceptions listed 18 U.S. Code § 2510, for they are contingent on two criteria which Officer Turner does not meet:

a. Officer Turner did not use a version of Freenet "*furnished to the subscriber or user by a provider of wire or electronic communication service*". 18 U.S. Code § 2510(5)(a)(i). Instead, Officer Turner used a modified version of the Network software, available only to sworn law enforcement officers, which was not publicly available. {Affidavit #31-33}.
b. Officer Turner was not using Freenet in the ordinary course of business. Ordinary Course of business would require the product to be used as designed and as delivered by the service provider. Instead, Officer Turner used a modified version, built and provided by law enforcement, with extra capabilities to monitor network traffic and intercept private communications.

20. Defendant was using a commercially available product and was only interacting with the Freenet product. Defendant was not interacting with another human nor was he communicating with another human. Therefore, Officer Turner was not a party to this conversation. Instead, Officer Turner was just reading the log generated by his customized wiretap program. Neither *On Lee v. United States* nor *Hoffa v. United States* apply because Defendant did not converse with any human, let alone a government person.

Electronic Surveillance

21. Officer Turner was not party to the conversation, but rather he was using the software to conduct electronic surveillance of Freenet communications. EO-12333 (Executive Order 12333, *United States Intelligence Activities* (1981) at 15, sec. 3.5(c)) defines:

22. ***Electronic Surveillance*** *means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.*

23. The meaning of *person* means "*every infant member of the species homo sapiens who is born alive and at any state of development*," 1 U.S. Code § 8. Officer Turner had a software program monitoring the communications (a modified version of Freenet). Software does not qualify as a *person* who can be party to a conversation. As such, this software program is not a *person* but a *thing*. Therefore, Officer Turner was conducting Electronic Surveillance using a *thing* (wiretap software) to monitor private communications without a warrant. Since software programs are not people, they cannot grant permission for someone else to record (or log) what is being

communicated. EO-12333 was codified into law in the 1986 Electronic Communications and Privacy Act, which prohibits wiretapping without a warrant, 18 U.S. Code § 2511, 18 U.S. Code § 2701, and 18 U.S. Code § 3121.

Pen Register Law

24. Freenet works to preserve the anonymity of its users. {Affidavit #5, 6} Yet Officer Turner used the modified version of the Network to extract IP addresses with a probability of having downloaded suspicious content. These IP addresses were logged. Officer Turner then went through a long process of submitting various administrative subpoenas to obtain the identity of the owner for the IP address. {Affidavit #68-69}. The name returned from these subpoenas was written on the request for an arrest warrant, and the resulting address was written on the request for a search warrant. However, Officer Turner did not obtain a warrant before beginning the process of unmasking the identity of the end user, violating 18 U.S. Code § 3121. The requirement for a warrant is explicitly stated in 18 U.S. Code § 2703(c)(1)(A)

> **(1)** A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
>
> **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ... (emphasis added)

25. A pen register is not just a device, but also a "process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is

transmitted." Use of a pen register process requires a warrant, 18 U.S. Code § 3121.

26. Officer Turner gives a detailed explanation of the route taken for a file block request. Once located, the file block would be returned along this same route. Officer Turner describes how a request goes out from User A to User B. If User B does not have the requested block, the request is forwarded to another user, say User M, and this request is forwarded up to 18 times. {Affidavit #15-17}. This route assists law enforcement to distinguish between a user that is the original requestor and one that has forwarded the request. {Affidavit #18}. The modified version of the software automatically logs this routing information and the number of times a request may be forwarded. {Affidavit #32-33}. However, any device or process which records routing information cannot be used unless a pen register warrant is obtained, for a pen register protects routing information. 18 U.S. Code § 3121. Since no such warrant was obtained prior to using this logging program, all information derived from this log should be suppressed.

27. An IP address is an Internet Protocol Address, which qualifies as an *address*. 18 U.S. Code § 3127(3). Just as a phone number (585-555-1212) is used for one phone to dial another so the users can communicate, an IP address (67.246.249.46) is a number computers use to "dial" each other and communicate. Tracing a phone number requires a warrant, *Smith v. Maryland,* 442 US 735 (1979). Identifying the owner of an email address requires a warrant, *McVeigh v. Cohen*, 983 F. Supp. 215 (D.D.C. 1998). An IP address is an "address" also protected by Fourth Amendment Law. A warrant was required, not just an administrative subpoena, 18 U.S. Code § 3121. The resulting name and address

obtained from the administrative subpoena should be suppressed. 18 U.S. Code § 2515.

28. Courts have broadly upheld a person's right to remain anonymous such as in a public blog or when posting a simple textbook, *Signature Mgmt. Team, LLC v. Doe*, 323 F. Supp. 3d 954 (E.D. Mich. 2018). Law enforcement must obtain a warrant to electronically track one's geographic location, *U.S. v. Jones,* 565 U.S. 400 (2012), but Defendant's home address was identified from electronic communications without any warrant. The DNI's federal policy document, *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information*, states "*Special authorization is required to obtain information protected by the Fourth Amendment*[3]." "*If the technique or method being considered seems to require specialized tradecraft or skills, or is typically used in clandestine ways, then that is an indicator that legal counsel should be consulted.*" No such Court review or authorization was obtained prior to using the modified version of the Network software tool to obtain IP address information.

Intent

29. As part of the user Freenet user agreement, the user agrees to provide Freenet a portion of the user's disk space to Freenet. {Affidavit #7} Freenet then will store whatever the system deems necessary to store there for efficient network operation, randomly distributing them on various user's

[3] Office of Director of National Intelligence (DNI), *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information* (July 2011), *at 6*

computers. {Affidavit #9}. Data is put on the user's computer, even if the user did not request it:

"Unlike other peer-to-peer networks, you as a user have little or no control over what is stored in your datastore. Instead, files are kept or deleted depending on how popular they are. This allows Freenet to be censorship-resistant. There is no "delete file" operation[4].

30. The Affidavit's simplistic wagon-wheel diagrams of the network gives the impression that users have knowledge of their directly connected nodes . A more accurate representation of any such network is a highway map of the country. Baltimore and Denver are on the same I-70, but you cannot drive between them without stopping. Files transmitted between these two cities will probably have an intermediate transmission point. There are large highways and small residential streets, but both are able to handle vehicle traffic at different capacities. If someone purchases a home on a quiet, residential street, they do not expect a parade of tanker trucks to flow in front of their home. Yet, if there is a major crash on the nearby freeway, traffic will be diverted onto their street to balance the traffic load. Similarly, if a user downloads Freenet for legitimate purposes, he has no control over what network balancing algorithm may decide to put on his computer's disk space. The Freenet algorithms add or delete files from the disk space according to the popularity of that file with others in the

[4] Freenetproject.org, Freenet Documentation, https://freenetproject.org/pages/documentation.html, Accessed January 2, 2023.

network and the transmission route between sender and receiver, not because the said user requested the file. Therefore, if a forensic search of a computer with Freenet finds a file, or file block, without any indication the user requested it, i.e., a relayer, this lacks criminal intent that the user himself download the file.

Modified Versions of Freenet are not Publicly Available

31. Officer Turner has implied that this modified version of Freenet built by law enforcement should be considered publicly available because Freenet source code is publicly available on a website. {Affidavit #6} Only software engineers can understand software, and only those with nefarious purposes would download this source code and modify it to do what law enforcement has done here – monitor network traffic to predict content transmitted. In order for something to be considered "publicly available", the information must be available to any member of the general public[5]. Note that this definition requires that the information, not just source code that is unintelligible to the average person, must be available to the general public. Therefore, the modified Freenet not publicly available, so it requires a warrant to use. Since no warrant was obtained prior to use, it was used in violation of laws defined in the Electronic Communications and Privacy Act of 1986.

Summary

[5] Office of Director of National Intelligence (DNI), *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information* (July 2011), *at 3 #1.*

32. Freenet provides a private electronic communication service to the public, just like phone companies. As a public communication service, its communications are protected by Fourth Amendment privacy laws, just like telephone companies, 18 U.S. Code § 2701(2)(a)(i). Phone companies manage a network of telephones with switchboards and routing software to properly route the communications to the intended recipient. Today's telephone communications not only include land lines and cell phones, but also include VoIP, Voice over IP (Internet Protocol). These VoIP phones calls allow people to make phone calls using their computer and the internet. These VoIP phone calls are also packed into small blocks to be transmitted over the same internet (IP) wires and pathways as Freenet. So how is a private VoIP phone call different than private file transfer using Freenet? The Fourth Amendment laws protecting phone calls also protect private file transfers.

WHEREFORE, defendant respectfully requests the Court to suppress all evidence seized by law enforcement from 117 Neuchatel Lane as referenced in the government's notice of intent to use evidence (exhibit A).

DATED: February 24, 2023

Respectfully submitted,

/s/James A. Napier

JAMES A. NAPIER, ESQ.